

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.</p>					
1. REPORT DATE (DD-MM-YYYY) 01-03-2017		2. REPORT TYPE Bibliography		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE Inside the Wire: American Security and Cyber Warfare				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Frances K. Scott				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) HQ USAFA/DFLIB-REF 2354 FAIRCHILD DRIVE, STE 3A22 USAF ACADEMY CO 80840-6214				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) DEPARTMENT OF THE AIR FORCE MCDERMOTT LIBRARY U.S. AIR FORCE ACADEMY USAF ACADEMY CO 80840-6214				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) Special Bibliography Series #119	
12. DISTRIBUTION/AVAILABILITY STATEMENT A					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT This bibliography supports the 58th Academy Assembly to be held at the United States Air Force Academy, 14-17 March 2017. This year's topic examines the policies, politics, and ethics of cyberspace and national security from a strategic perspective. It challenges assumptions about cyber capabilities, cyber war, international relations, privacy, and considers how the US uses cyber to further national security objectives.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code)
U	U	U	UU	38	

**SPECIAL
BIBLIOGRAPHY
SERIES**

Inside the Wire: American Security and Cyber Warfare



March 2017

**SPECIAL
BIBLIOGRAPHY
SERIES**

NO. 119



DEPARTMENT OF THE AIR FORCE

McDERMOTT LIBRARY
UNITED STATES AIR FORCE ACADEMY
USAF ACADEMY, COLORADO 80840-6214



INTRODUCTION

This *Special Bibliography Series*, Number 119, “Inside the Wire: American Security and Cyber Warfare,” was developed by the McDermott Library’s Social Sciences Bibliographer and Reference Librarian, Frances K. Scott, in support of the 58th Academy Assembly to be held at the United States Air Force Academy, 14-17 March 2017.

Most items cited in the bibliography are included in the McDermott Library’s collections, including on-line databases. This year’s topic examines the policies, politics, and ethics of cyberspace and national security from a strategic perspective. It challenges assumptions about cyber capabilities, cyber war, international relations, privacy, and considers how the US uses cyber to further national security objectives. If you are a participant in this year’s Academy Assembly (the Academy’s oldest continuing annual event), we welcome you to your United States Air Force Academy. We hope that your stay in the Colorado Springs area will be rewarding and enjoyable and that you find this year’s topic intellectually challenging.

This bibliography available free of charge via the McDermott Library’s web site. Comments may be sent to:

HQ USAFA/DFLIB-REF
Attn: Ms. Frances K. Scott
Social Sciences Bibliographer
2354 Fairchild Drive, Ste 3C9
USAF Academy CO 80840-6214

This (and all the previous issues of the *Special Bibliography Series*) are available on the library’s web site at:

https://afac.ent.sirsi.net/client/en_US/cadet/?rm=SPECIAL+BIBLIO00%7C%7C%7C1%7C%7C%7C0%7C%7C%7Ctrue

Comments about this year’s bibliography or other library programs should be sent to the address above.

EDWARD A. SCOTT, Ph.D.
Associate Dean and Director,
McDermott Library
March 2017

TABLE OF CONTENTS

I.	DIRECTOR'S PICKS.....	1
II.	CYBERSPACE DOMESTIC TOPICS.....	2
III.	COMPUTER ISSUES.....	5
IV.	FOREIGN POLICY INCLUDING POLITICS.....	8
V.	INTELLIGENCE COMPONENTS.....	10
VI.	INTERNATIONAL AND NATIONAL SECURITY.....	13
VII.	INTERNATIONAL RELATIONS INCLUDE RUSSIA AND CHINA.....	19
VIII.	LEGAL REGULATIONS AND IMPLICATIONS.....	23
IX.	FINANCIAL AND ECONOMIC AREAS.....	27
X.	CYBERWARFARE.....	29
XI.	WEBSITES.....	34

I. DIRECTOR'S PICKS READING LIST
Books, Government Documents, and Report Literature

- Healey, Jason. "The Five Futures of Cyber Conflict and Cooperation." *Atlantic Council*. December 14, 2011. <http://www.atlanticcouncil.org/publications/issue-briefs/the-five-futures-of-cyber-conflict-and-cooperation>
- Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (May 2011): 49-60.
- Landwehr, C. E. Landwehr, "History of US Government Investments in Cybersecurity Research: A Personal Perspective," *2010 IEEE Symposium on Security and Privacy*, Oakland, (2010):14-20.
- Lindsay, Jon R. "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack." *Journal of Cybersecurity* 1, no. 1(September 2015): 53-67.
- Mills, John R. "The Key Terrain of Cyber." *Georgetown Journal of International Affairs*, (2012): 99-107. http://journal.georgetown.edu/wp-content/uploads/2015/07/gj12712_Mills-CYBER-2012.pdf.
- Rainie, Lee. "The State of Privacy in Post-Snowden America." *Fact Tank*. (September 21, 2016). <http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/#>.
- Raymond, David, et al. "Key Terrain in Cyberspace: Seeking the Higher Ground." International Conference on Cyber Conflict, (3-6 June, 2014). <http://ieeexplore.ieee.org/document/6916409/>
- Posner, Richard A. "Privacy, Surveillance, and Law," *University of Chicago Law Review* 75, no. 1(Winter 2008): 245-260.
- Rid, Thomas, and Peter McBurney. "Cyber Weapons." *The RUSI Journal* 157 no. 1(February 2012): 6-13.
- Warner, Michael. Cybersecurity: A Pre-history. *Intelligence and National Security* 27, no. 5(October 2012): 781-799.
- Warner, Michael, and Michael Good. "Notes on Deterrence in Cyberspace." *Georgetown Journal of International Affairs* (June 2015): 71-78. http://journal.georgetown.edu/wp-content/uploads/2015/07/gjia13006_Warner-CYBER-III.pdf

II. CYBERSPACE DOMESTIC TOPICS

Books, Government Documents, and Report Literature

- Barack Obama Administration. *Presidential Policy Directive/PPD-20*. White House, 2012.
(<https://fas.org/irp/offdocs/ppd/ppd-20.pdf>)
- Betz, David J. and Timothy C Stevens. *Cyberspace and the State: Towards a Strategy for Cyberpower*. Abingdon; New York: Routledge, 2011.
(HM 851 .B485 20141)
- Jarvis, Lee, Stuart Keith MacDonald, and Thomas M. Chen. *Terrorism Online: Politics, Law and Technology*. Routledge studies in conflict security and technology. London: Routledge, 2015.
(HV 6773.15 .C97 T47 2015eb)
- Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016.
(HV 6773.15 .C97 K37 2016)
- Kay, Sean. *Global Security in the Twenty-First Century: The Quest for Power and the Search for Peace*. 2nd ed. Lanham: Rowman & Littlefield, 2012.
(JZ 5588 .K39 2012)
- Koppel, Ted. *Lights Out: A Cyberattack, a Nation Unprepared, Surviving the Aftermath*. New York: Crown, 2015.
(TK 1025 .K67 2015)
- Kostopoulos, George K. *Cyberspace and Cybersecurity*. Boca Raton: CRC, 2013.
(TK 5105.59 .C94 2013)
- Russell, Alison Lawlor. *Cyber Blockades*. Washington: Georgetown UP, 2014.
(HV 6773.15 .C97 R87 2014)
- United States. Congress. House. Committee on Homeland Security. Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies. *Facilitating Cyber Threat Information Sharing and Partnering With the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities*. Hearing. 113 Cong., 1st sess. Washington: GPO, 2013.
(Gov Doc Y 4.H 75:113-17)

JOURNALS

- Bajaj, Kamlesh. "Cyberspace As Global Commons: The Challenges." *Dataquest* 30, no. 7(April 2012): 40-4.
- Bronk, Christopher, Cody Monk, and John Villasenor. "The Dark Side of Cyber Finance." *Survival* 54, no. 2(April 2012-May 2012): 129-42.
- Bryant, William D. "Cyberspace Superiority A Conceptual Model." *Air & Space Power Journal* 27, no. 6(November 2013-December 2013): 25-44.

- Cai, Cuihong, and Diego Dati. "Words Mightier Than Hacks: Narratives of Cyberwar in the United States and China." *Asian Perspective: SPECIAL ISSUE* 39, no. 3(July 2015-September 2015): 541-53.
- Caplan, Nathalie. "Cyber War: The Challenge to National Security." *Global Security Studies* 4, no. 1(Winter 2013): 3-115.
- Condrón, Sean M. "Getting It Right: Protecting American Critical Infrastructure in Cyberspace." *Harvard Journal of Law & Technology* 20, no. 2(Spring 2007): 403-22.
- Creedon, Madelyn R. "Space and Cyber: Shared Challenges, Shared Opportunities." *Strategic Studies Quarterly* 6, no. 1(Spring 2012): 3-8.
- Cser, Orsolya. "The Role and Security of Money From the Aspect of Cyber Warfare." *AARMS: Academic & Applied Research in Military & Public Management Science*. 14, no. 3(January 2015): 331-42.
- Demchak, Chris C., and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* 5, no. 1(Spring 2011): 32-61.
- Dobrian, Joseph. "Are You Sitting on a Cyber Security Bombshell?" *Journal of Property Management* 80, no. 5(September 2015-October 2015): 8-11.
- Ebert, Hannes, and Tim Maurer. "Contested Cyberspace and Rising Powers." *Third World Quarterly* 34, no. 6(July 2013): 1054-74.
- Gartzke, Erik, and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24, no. 2(April 2015-June 2015): 316-48.
- Greiman, Virginia A. "National Intelligence, Corporate Competitiveness and Privacy Rights: Co-Existing in Cyberspace." *Global Studies Journal* 9, no. 3(2016): 43-56.
- Gross, Jessica R. "Hacked and Be Hacked: A Framework for the United States to Respond to Non-State Actors in Cyberspace." *California Western International Law Journal* 46, no. 2(Spring 2016): 109-45.
- Gross, Oren. "Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents." *Cornell International Law Journal* 48, no. 3(Fall 2015): 481-511 .
- Jakobi, Anja P. "Non-State Actors and Global Crime Governance: Explaining the Variance of Public-Private Interaction." *British Journal of Politics and International Relations* 18, no. 1(February 2016): 72-89.
- Jensen, Eric Talbot. "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense." *Stanford Journal of International Law* 38(2002): 207-41.
- Johnson, Phillip A. "Is It Time for a Treaty on Information Warfare?" *International Law Studies* 76, no. 439-455(2002).
- Lee, Robert M. "The Interim Years of Cyberspace." *Air & Space Power Journal* 27, no. 1(January 2013-February 2013): 58-79.
- Lincoln, Bonner E. "Defending Our Satellites." *Air & Space Power Journal* 29, no. 6(November 2015-December 2015): 74-82.

- Lynn III, William J. "Defending a New Domain." *Foreign Affairs* 89, no. 5(September 2010-October 2010): 97-108.
- Nielsen, Suzanne C. "Pursuing Security in Cyberspace: Strategic and Organizational Challenges." *Orbis: A Journal of World Affairs* 56, no. 3(Summer 2012): 336-56.
- Nojeim, Gregory T. "Cybersecurity and Freedom on the Internet." *Journal of National Security Law & Policy* 4, no. 1(August 2010): 119-37.
- Nye, Joseph S. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4(Winter 2011): 18-39.
- Roesener, G., Carl Bottolfson, and Gerry Fernandez. "Policy for US Cybersecurity." *Air & Space Power Journal* 28, no. 6(November 2014-December 2014): 38-54.
- Rudner, Martin. "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge." *International Journal of Intelligence and Counterintelligence* 26, no. 3(May 2013): 453-81.
- Serrano, Antonio Segura. "Cybersecurity: Towards a Global Standard in the Protection of Critical Information Infrastructures." *European Journal of Law and Technology* 6, no. 3(2015): 1-121.
- Shea, Jamie. "How Is NATO Dealing with Emerging Security Challenges?" *Georgetown Journal of International Affairs* 14, no. 2(Summer 2013-Fall 2013): 193-201.
- Tereshchenko, Natalia. "US Foreign Policy Challenges of Non-State Actors' Cyber Terrorism Against Critical Infrastructure." *International Journal of Cyber Warfare and Terrorism* 2, no. 4(2012): 28-48.
- Van Epps, Geoff. "Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain." *Connections* 12, no. 4(Fall 2013): 15-50.
- Wedgwood, Ruth G. "Proportionality Cyberwar, and the Law of War." *International Law Studies* 76(2002): 219-32.
- Whyte, Christopher. "Power and Predation in Cyberspace." *Strategic Studies Quarterly* 9, no. 1(Spring 2015): 100-118.
- .

III. COMPUTER ISSUES

Books, Government Documents, and Report Literature

- Arquilla, John and David F. Ronfeldt. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND, 2001.
(REPORT LITERATURE RAND MR-1382-OSD)
- Coleman, E. Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London; New York: Verso, 2014.
(HV 6773 .C646 2014)
- Denning, Dorothy Elizabeth Robling. *Information Warfare and Security*. New York; Reading: ACM; Addison-Wesley, 1999.
(U 163 .D46 1999)
- Hafner, Katie and John Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster, 1991.
(QA 76.9 .A25 H34 1991)
- Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge UP, 2007.
(U 163 .L534 2007)
- Parker, Tom, et al. *Cyber Adversary Characterization: Auditing the Hacker Mind*. Rockland: Syngress, 2004.
(QA 76.9 .A25 C93 2004eb)
- Rosenzweig, Paul. *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. Changing face of war. Santa Barbara: Praeger, 2012.
(U163 .R68 2012)
- Schwartau, Winn. *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age*. 2nd ed. New York: Thunder's Mouth, 1996.
(QA 76.9 .A25 S354 1996)
- Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: PublicAffairs, 2016.
(JZ 1254 .S44 2016)
- Sterling, Bruce. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam, 1992.
(HV 6773.2 .S74 1992)
- United States. Congress. House. Committee on Science, Space and Technology 2011 Subcommittee on Research and Technology. *The Expanding Cyber Threat*. Hearing. 114th Cong., 1st sess. Washington: GPO, 2015.
(Gov Doc Y 4.SCI 2:114-2)
- Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown, 2014.
(UG 593 .Z48 2014)

JOURNALS

- Arquilla, John and David Ronfeldt. "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2(1993): 141-65.
- Axelrod, Robert and Iliev Rumen. "Timing of Cyber Conflict." *Proceedings of the National Academy of Sciences* 111, no. 4(January 2014): 1298-303.
- Benson, David C. "Why the Internet Is Not Increasing Terrorism." *Security Studies* 23, no. 2(May 2014): 293-328.
- Deibert, Ron. "Cyberspace under Siege." *Journal of Democracy* 36, no. 3(July 2015): 64-78.
- Doneda, Danilo and Virgilio A.F. Almeida. "Privacy Governance in Cyberspace." *IEEE Internet Computing* 19, no. 3(2015): 50-3.
- Farwell, James P., and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival* 53, no. 1(February 2011-March 2011): 23-40.
- Herr, Trey and Paul Rosenzweig. "Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model." *Journal of National Security Law & Policy* 8, no. 2(October 2015): 301-19.
- Hollis, Duncan B. "Why States Need an International Law for Information Operations." *Lewis & Clark Law Review* 11, no. 4(Winter 2007): 1023-61.
- Lin, Herbert. "A Virtual Necessity: Some Modest Steps Toward Greater Cybersecurity ." *Bulletin of the Atomic Scientists* 68, no. 5(September 2012): 75-87.
- Lin, Herbert S. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law & Policy* 4, no. 1(2010): 63-86.
- Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3(July 2013-September 2013): 365-404.
- Lipner, Steven B. "The Birth and Death of the Orange Book." *IEEE Annals of the History of Computing* 37, no. 2(April 2015-June 2015): 19-31.
- Rid, Thomas and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1-2(2015): 4-37.
- Robertson Jr, Horace B. "Self-Defense against Computer Network Attack under International Law." *International Law Studies* 76(2002): 121-45.
- Watts, Sean. "Low-Intensity Computer Network Attack and Self-Defense." *International Law Studies* 87, no. 1(2011): 59-87.
- Williams, Robert D. "(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action." *George Washington Law Review* 79, no. 4(June 2011): 1162-200.
- Wood, Colin. "Mission Impossible?" *Government Technology* 27, no. 8(2014): 16-20.

Yost, Jeffrey R. "The Origin and Early History of the Computer Security Software Products Industry."
IEEE Annals of the History of Computing 37, no. 2(April 2015-June 2015): 46-58.

IV. FOREIGN POLICY INCLUDING POLITICS

Books, Government Documents, and Report Literature

- Betz, David J. and Timothy C Stevens. *Cyberspace and the State: Towards a Strategy for Cyberpower*. Abingdon; New York: Routledge, 2011.
(HM 851 .B485 20141)
- Brantly, Aaron Franklin. *The Decision to Attack: Military and Intelligence Cyber Decision-Making*. Studies in security and international affairs. Athens: U of Georgia P, 2016.
(U 163 .B69 2016eb)
- Cavelty, Myriam Dunn. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. CSS studies in security and international relations. London; New York: Routledge, 2008.
(QA 76.9 .A25 D87 2008eb)
- Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge: MIT P, 2012.
(JZ 1254 .C47 2012)
- Jasper, Scott, ed. *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*. Washington: Georgetown UP, 2012.
(JZ 6005 .C66 2012)
- . *Securing Freedom in the Global Commons*. Stanford: Stanford Security Studies, 2010.
(UA 10.5 .S3725 2010)
- Karatzogianni, Athina, ed. *Cyber-Conflict and Global Politics*. Contemporary security studies. New York: Routledge, 2009.
(HM 851 .C924 2009eb)
- Price-Smith, Andrew T. ed. *Rising Threats, Enduring Challenges: Readings in U.S. Foreign Policy*. New York: Oxford UP, 2015.
(E 183.7 .R67 2015)
- Schmidt, Lara. *Perspective on 2015 DoD Cyber Strategy*. Santa Monica: RAND, 2015.
(<http://www.dtic.mil/docs/citations/ADA621794>)
- Smith, Douglas S. *Securing Cyberspace: Approaches to Developing an Effective Cyber-Security Strategy*. Carlisle Barracks: U.S. Army War College, 2011.
(<http://www.dtic.mil/dtic/tr/fulltext/u2/a565052.pdf>)
- United States. Congress. House. Committee on Armed Services. Subcommittee on Intelligence, Emerging Threats and Capabilities. *Information Technology and Cyber Operations: Modernization and Policy Issues in a Changing National Security Environment*. Hearing. 113th Cong., 2d sess. Washington: GPO, 2014.
(Gov Doc Y 4.AR 5/2 A:2013-2014/87)

JOURNALS

- "Core Considerations Regarding Cybersecurity, Sovereignty, and U.S. Foreign Policy." *American Foreign Policy Interests* 36, no. 5(September 2014-October 2014): 332-3.
- Chenou, Jean-Marie. "From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-Stakeholderism, and the Institutionalisation of Internet Governance in the 1990s." *Globalizations* 11, no. 2(April 2014): 205-23.
- Cornish, Paul. "Governing Cyberspace through Constructive Ambiguity." *Survival* 57, no. 3(June 2015): 153-76.
- Dipert, Randall R. "The Ethics of Cyberwarfare." *Journal of Military Ethics* 9, no. 4(December 2010): 384-410.
- . "Other-Than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law, and Policy." *Journal of Military Ethics* 12, no. 1(April 2013): 34-53.
- Flowers, Angelyn and Sherali Zeadally. "US Policy on Active Cyber Defense." *Journal of Homeland Security & Emergency Management* 11, no. 2(June 2014): 289-308.
- Foster, William and Hannah Thoreson. "How to Create a World Financial Community Resilient to Cyber-Espionage and Hacking?" *Security Index: A Russian Journal on International Security* 19, no. 4(December 2013).
- Johanson, Derek. "The Evolving U.S. Cybersecurity Doctrine." *Security Index: A Russian Journal on International Security* 19, no. 4(December 2013): 37-50.
- Landis, Benjamin L. "A National Defense Policy for the Twenty-First Century." *American Diplomacy* (October 2010): 1-6.
- Liu, Shih-Diing. "The Cyberpolitics of the Governed." *Inter-Asia Cultural Studies* 14, no. 2(June 2013): 252-71.
- Nocetti, Julien. "Contest and Conquest: Russia and Global Internet Governance." *International Affairs*. 91, no. 1(January 2015): 110-30.
- Sheldon, John B. "Geopolitics and Cyber Power: Why Geography Still Matters." *American Foreign Policy Interests* 36, no. 5(September 2014-October 2014): 286-93.
- Tereshchenko, Natalia. "US Foreign Policy Challenges of Non-State Actors' Cyber Terrorism Against Critical Infrastructure." *International Journal of Cyber Warfare and Terrorism* 2, no. 4(2012): 28-48.
- Whyte, Christopher. "Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea." *Comparative Strategy* 35, no. 2(2016): 93-102.

V. INTELLIGENCE COMPONENTS

Books, Government Documents, and Report Literature

- Cyber Intelligence: Setting the Landscape for an Emerging Discipline*. Arlington: Intelligence and National Security Alliance, 2011.
(images.magnetmail.net/images/clients/INSA/attach/INSA_CYBER_INTELLIGENCE_2011.pdf
)
- Bamford, James. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. New York: Anchor, 2002.
(UB 256 .U6 B36 2002)
- . *The Puzzle Palace: A Report on America's Most Secret Agency*. Harmondsworth, Middlesex; New York: Penguin, 1983.
(UB 251 .U5 B35 1983)
- Betts, Richard K. *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia UP, 2007.
(JK 468 .I6 B44 2007)
- Cappelli, Dawn M., Andrew P. Moore, and Randall F. Trzeciak. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Upper Saddle River: Addison-Wesley, 2102.
(On order)
- Cyber Intelligence Task Force. *Operational Levels of Cyber Intelligence*. Arlington: Intelligence and National Security Alliance, 2013.
([file:///C:/Users/Frances.Scott/Downloads/Operational%20Levels%20of%20Cyber%20Intelligence%20\(6\).pdf](file:///C:/Users/Frances.Scott/Downloads/Operational%20Levels%20of%20Cyber%20Intelligence%20(6).pdf))
- Kahn, David. *The Codebreakers: The Story of Secret Writing*. Rev. ed. New York: Scribner, 1996.
(Z 103 .K28 1996)
- Koppel, Ted. *Lights Out: A Cyberattack, a Nation Unprepared, Surviving the Aftermath*. New York: Crown, 2015.
(TK 1025 .K67 2015)
- Rovner, Joshua. *Fixing the Facts: National Security and the Politics of Intelligence*. Cornell studies in security affairs. Ithaca: Cornell UP, 2011.
(JK 468 .I6 R687 2011)
- Stoll, Clifford. *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*. New York: Doubleday, 1989.
(UB 271 .R92 H477 1989)
- Yardley, Herbert O. *The American Black Chamber*. Indianapolis: Bobs-Merrill, 1931.
(D 639 .S7 Y3 1931)

JOURNALS

- Brown, Gary D. "Spying and Fighting in Cyberspace: What Is Which?" *Journal of National Security Law & Policy* 8, no. 3(March 2016): 1-22.
- Burton, Joe. "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation." *Defence Studies* 15, no. 4(December 2015): 297-319.
- Colesniuc, Dan, and Marian Turlei. "Cyberspace Semantics at NATO Level." *Romanian Military Thinking* 2(April 2015-June 2015): 83-94.
- Crane, David M. "Fourth Dimensional Intelligence Thoughts on Espionage, Law, and Cyberspace." *International Law Studies* 76(2002): 311-21.
- Dunlap, Jr. Charles J. "Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy." *International Law Studies* 76(2002): 353-73.
- Eichensehr, Kristen E. "The Cyber-Law of Nations." *Georgetown Law Journal* 103, no. 2(January 2015): 317-80.
- Inkster, Nigel. "Chinese Intelligence in the Cyber Age." *Survival* 55, no. 1(February 2013-March 2013): 45-66.
- Jung ho, Eom. "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace." *International Journal of Software Engineering And Its Applications* 8, no. 9(September 2014): 137-46.
- Lotrionte, Catherine. "Countering State-Sponsored Cyber Economic Espionage Under International Law." *North Carolina Journal of International Law and Commercial Regulation* 40, no. 2(Winter 2015): 443-541.
- Lubell, Noam. "Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?" *International Law Studies* 89(2013): 252-75.
- Maness, Ryan C., and Brandon Valeriano. "The Impact of Cyber Conflict on International Interactions." *Armed Forces & Society* 42, no. 2(April 2016): 301-23.
- Nastasiu, Cătălin-Ionuț. "Cyber Security Strategies in the Internet Era." *Scientific Research & Education In The Air Force - AFASES* 2(2016): 619-24.
- Schmitt, Michael N. "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law." *Virginia Journal Of International Law* 54, no. 3(August 2014): 698-732.
- . "The Law of Cyber Targeting." *Naval War College Review* 68, no. 2(Spring 2015): 10-29.
- Skinner, Christian Parajon. "An International Law Response to Economic Cyber Espionage." *Connecticut Law Review* 46, no. 4(May 2014): 1165-207.
- Smith, Jeffrey H. and Gordon N. Lederman. "Weapons Like to Lightning"! US Information Operations and US Treaty Obligations." *International Law Studies* 76(2002): 375-93.

Williams, Robert D. "(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action."
George Washington Law Review 79, no. 4(June 2011): 1162-200.

VI. INTERNATIONAL AND NATIONAL SECURITY

Books, Government Documents, and Report Literature

- Andress, Jason, Steve Winterfeld, and Russ Rogers. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Boston: Elsevier, 2011.
(U 163 .A64 2011)
- Barker, Cody L., ed. *Cyberspace Threat Landscape: Overview, Response Authorities, and Capabilities*. Internet Theory, Technology and Applications. New York: Nova Science, 2015.
(HV 6773.15 .C97 C934 2015)
- Carr, Madeline. *US Power and the Internet in International Relations: The Irony of the Information Age*. Basingstoke, Hampshire: Palgrave Macmillan, 2016.
(JZ 1254 .C37 2016eb)
- Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Ecco, 2012.
(HV 6773.2 .C53 2010)
- de Silva, Eugenie. *National Security and Counterintelligence in the Era of Cyber Espionage*. Advances in digital crime forensics and cyber terrorism (ADCFCF). Hershey: Information Science Reference, 2016.
- Demchak, Chris C. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Studies in security and international affairs. Athens: U of Georgia P, 2011.
(U 163 .D36 2011)
- Dunn-Cavelty, Myriam. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. CSS studies in security and international relations. Abingdon; New York: Routledge, 2008.
(QA 76.9 .A25 D87 2008eb)
- Guiora, Amos N. *Cybersecurity .Geopolitics, Law, and Policy*. Boca Raton: CRC P, 2016.
(On order)
- Jarmon, Jack A. *The New Era in U.S. National Security: An Introduction to Emerging Threats and Challenges*. Lanham: Rowman & Littlefield, 2014.
(UA 23 .J35 2014)
- Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Washington: National Defense U, Center for Technology and National Security Policy, 2009.
(UA 23 .C929 2009)
- Libicki, Martin. *Cyberspace in Peace and War*. Annapolis: Naval Institute P, 2016.
(U 163 .L54 2016)
- Rovner, Joshua. *Fixing the Facts: National Security and the Politics of Intelligence*. Cornell studies in security affairs. Ithaca: Cornell UP, 2011.
(JK 468 .I6 R687 2011)

- Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown, 2012.
(E 907 .S26 2012)
- Singer, P. W. Peter Warren, and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. What everyone needs to know. Oxford; New York: Oxford UP, 2014.
(QA 76.9 .A25 S562 2014)
- Smith, Douglas S. *Securing Cyberspace: Approaches to Developing an Effective Cyber-Security Strategy*. Carlisle Barracks: U.S. Army War College, 2011.
(<http://www.dtic.mil/get-tr-doc/pdf?AD=ADA565052>)
- Stevens, Tim. *Cyber Security and the Politics of Time*. Cambridge: Cambridge UP, 2016.
(JZ 1254 .S74 2015eb)
- Tehan, Rita. *Cybersecurity: Authoritative Reports and Resources*. Washington: Congressional Research Service, 1925.
(REPORT LITERATURE ADA 5888715)(<http://www.dtic.mil/get-tr-doc/pdf?AD=ADA588715>)
- United States. Cong. House. Committee on Armed Services. Strategic Forces Subcommittee. *Assuring Aassured Access to Space*. Hearing. 114th Cong., 1st sess. Washington: GPO, 2015.
(Gov Doc Y 4.AR 5/2 A:2015-2016/21)
- . ---. ---. Committee on Armed Services. Subcommittee on Emerging Threats and Capabilities. *Cyber Operations: Improving the Military Cybersecurity Posture in an Uncertain Threat Environment*. Hearing. 114th Cong., 1st sess. Washington: GPO, 2015.
(Gov Doc Y 4.AR 5/2 A:2015-2016/19)
(<http://purl.fdlp.gov/GPO/gpo63204http://www.gpo.gov/fdsys/pkg/CHRG-114hhr94221/pdf/CHRG-114hhr94221.pdf>)
- . ---. ---. Committee on Armed Services. Subcommittee on Intelligence, Emerging Threats and Capabilities. *Information Technology and Cyber Operations: Modernization and Policy Issues in a Changing National Security Environment*. Hearing. 113th Cong., 2d sess. Washington: GPO, 2014.
(Gov Doc Y 4.AR 5/2 A:2013-2014/87)
- . ---. ---. Committee on Foreign Affairs. *Cyber War: Definitions, Deterrence, and Foreign Policy*. Hearing. 114th Cong., 1st sess. Washington: GPO, 2015.
(Gov Doc Y 4.F 76/1:114-106)(<http://purl.fdlp.gov/GPO/gpo63802>)
- . ---. Senate. Committee on Commerce, Science and Transportation. *The Partnership Between NIST and the Private Sector: Improving Cybersecurity*. Hearing. 113th Cong., 1st sess. Washington: GPO, 2013.
(Gov Doc Y 4.C 73/7:S.HRG.113-285) (<https://www.gpo.gov/fdsys/pkg/CHRG-113shrg88081/pdf/CHRG-113shrg88081.pdf>)
- . ---. ---. Committee on Foreign Relations. Subcommittee on East Asia, the Pacific and International Cybersecurity Policy. *Cybersecurity: Setting the Rules for Responsible Global Cyber Behavior*. Hearing. 114th Cong., 1st sess. Washington: GPO, 2015.
(Gov Doc Y 4.F 76/2:S.HRG.114-76)(<http://purl.fdlp.gov/GPO/gpo63172>)

Weimann, Gabriel. *Terrorism in Cyberspace: The Next Generation*. Washington; New York: Woodrow Wilson Center; Columbia UP, 2015.
(On order)

Yannakogeorgos, Panayotis A., and Adam Lowther, eds. *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Boca Raton: Taylor & Francis, 2014.
(U 163 .C625 2014)

JOURNALS

Aleksandrowicz, Tomasz R. "Cyberspace As a Source of Threat to National Security: An Attempt to Conceptualize the Problem." *International Security* 7, no. 1(January 2015-June 2015): 187-204.

Andress, Jason. "Working with Indicators of Compromise." *ISSA Journal* (May 2015): 14-20.
Call Number: (c.ymcdn.com/sites/www.issa.org/resource/resmgr/journalpdfs/feature0515.pdf)

Archuleta, Brandon J. "Rediscovering Defense Policy: A Public Policy Call to Arms." *Policy Studies Journal* 44(May 2016): S50-S69.

Armenchev, Ilina, and Stefko Smolenov. "From Real Cyber Conflict through Wishful Cyber Security to (Un) Likely Cyber Peace." *Revista Academiei Fortelor Terestre* 20, no. 3(September 2015): 259-66.

Balushi, Taiseera Al, Saqib Ali, and Osama Rehman. "Economics of Cyber Security and the Way Forward." *International Journal of Cyber Warfare & Terrorism* 6, no. 4(October 2016-December 2016): 41-57.

Baumbauer, Derek E. "Ghost in the Network." *University of Pennsylvania Law Review* 162, no. 5(April 2014): 1011-91.

Berriz, Cristina. "Cybersecurity and United States Policy Issues." *Global Security Studies* 5, no. 3(2014): 35-40.

Burton, Joe. "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation." *Defence Studies* 15, no. 4(December 2015): 297-319.

Butler, Bob and Irving Lachow. "Multilateral Approaches for Improving Global Security in Cyberspace." *Georgetown Journal of International Affairs* (2012): 5-14.

Caplan, Nathalie. "Cyber War: The Challenge to National Security." *Global Security Studies* 4, no. 1(Winter 2013): 3-115.

Choucri, Nazli and Daniel Goldsmith. "Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security." *Bulletin of the Atomic Scientists* 68, no. 2(March 2012): 70-78.

Choucri, Nazli and David D. Clark. "Who Controls Cyberspace." *Bulletin of the Atomic Scientists* 69, no. 5(September 2013): 21-31.

Cimbala, Stephen J. "Nuclear Deterrence in Cyber-Ia." *Air & Space Power Journal* 30, no. 3(Fall 2016): 54-63.

- Colesniuc, Dan, and Marian Turlei. "Cyberspace Semantics at NATO Level." *Romanian Military Thinking* 2(April 2015-June 2015): 83-94.
- Deibert, Ronald J., and Masashi Crete-Nishihata. "Global Governance and the Spread of Cyberspace Controls." *Global Governance* 18, no. 3(July 2012-September 2012): 339-61.
- Demidov, Oleg. "No Peace No War 2015: An Outlook for Cyberspace and Global Security." *Security Index: A Russian Journal on International Security* 20, no. 3-4(September 2014-December 2014): 1-4.
- DeNardis, Laura. "The Internet Design Tension Between Surveillance and Security." *IEEE Annals of the History of Computing* 37, no. 2(April 2015-June 2015): 72-83.
- Devost, Matthew, Brian K. Houghton, and Neal Allen Pollard. "Information Terrorism: Political Violence in the Information Age." *Terrorism and Political Violence* 9, no. 1(Spring 1997): 72-83.
- Dunn Cavelty, Myriam. "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse." *International Studies Review* 15, no. 1(March 2013): 105-22.
- Gable, Kelly A. "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction As a Deterrent." *Vanderbilt Journal of Transnational Law* 43, no. 1(January 2010): 57-118.
- Greiman, Virginia A. "National Intelligence, Corporate Competitiveness and Privacy Rights: Co-Existing in Cyberspace." *Global Studies Journal* 9, no. 3(2016): 43-56.
- Guittton, Clement. "Cyber Insecurity As a National Threat: Overreaction from Germany, France and the UK?" *European Security* 22, no. 1(January 2013): 21-35.
- Hansen, Lena. "Theorizing the Image for Security Studies: Visual Securitization and the Muhammad Cartoon Crisis." *European Journal of International Relations* 17, no. 1(March 2011): 51-74.
- Hansen, Lena, and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53, no. 4(December 2009): 1155-75.
- Hathaway, Melissa E. "Connected Choices: How the Internet Is Challenging Sovereign Decisions [PANEL 1]." *American Foreign Policy Interests* 36, no. 5(September 2014-October 2014): 300-13.
- Hathaway, Melissa E. "PANEL 1: Connected Choices: The Internet and Sovereign Decision Making." *American Foreign Policy Interests Supplement* 2-3(January 2015-February 2015): 2-3.
- Heidenreich, John. "The Privacy Issues Presented by the Cybersecurity Information Sharing Act." *North Dakota Law Review* 91, no. 2(2015): 395-410.
- Hollis, Duncan B. "An E-SOS for Cyberspace." *Harvard International Law Journal* 52, no. 2(Summer 2011): 373-432.
- Hurwitz, Roger. "PANEL 3: The Play of States: Norms and Security in Cyberspace." *American Foreign Policy Interests Supplement*(January 2015-February 2015): 7-15.

- . "The Play of States: Norms and Security in Cyberspace." *American Foreign Policy Interests* 36, no. 5(September 2014-October 2014): 322-31.
- Ilves, Luukas K., et al. "European Union and NATO Global Cybersecurity Challenges." *PRISM Security Studies Journal* 6, no. 2(2016): 127-41.
- Ivanov, Galin R. "The Cybersecurity of Automated Control Systems As a Key Component of National Security." *Journal of Defense Resources Management* 7, no. 2(October 1916): 91-96.
- Jupillat, Nicolas. "Armed Attacks in Cyberspace: The Unseen Threat to Peace and Security That Redefines the Law of State Responsibility." *University of Detroit Mercy Law Review* 92, no. 2(Spring 2015): 115-30.
- Kallberg, Jan, and Bhavani Thuraisingham. "State Actors' Offensive Cyberoperations: The Disruptive Power of Systematic Cyberattacks." *IT Professional* 15, no. 3(May 2013-June 2013): 32-5.
- Keen, Major Jason F. "Conventional Military Force As a Response to Cyber Capabilities on Sending Packets and Receiving Missiles." *Air Force Law Review* 73(2915): 111-50.
- Kim, Sangbae. "Cyber Security and Middle Power Diplomacy: A Network Perspective." *The Korean Journal of International Studies* 12, no. 2(December 2014): 323-52.
- Kleinberg, Howard, et al. "Building a Theoretical Basis for Cyber Security Best Practices." *Annals of the MS in Computer Science and Information Systems at UNC Wilmington* 9, no. 2(Fall 2015): Paper 12.
Call Number: (<http://csb.uncw.edu/mscsis/complete/pdf/KleinbergHoward.pdf>)
- Kremer, Jens. "Policing Cybercrime or Militarizing Cybersecurity? Security Mindsets and the Regulation of Threats From Cyberspace." *Information & Communications Technology Law* 23, no. 3(October 2014): 220-237.
- Kshetri, Nir. "Cybercrime and Cyber-Security Issues Associated with China: Some Economic and Institutional Considerations." *Electronic Commerce Research* 13, no. 1(March 2013): 41-69.
- Lawson, Sean. "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats." *Journal of Information Technology & Politics* 10, no. 1(2013): 86-103.
- Lincoln, Bonner E. "Defending Our Satellites." *Air & Space Power Journal* 29, no. 6(November 2015-December 2015): 74-82.
- Lynn III, William J. "Defending a New Domain." *Foreign Affairs* 89, no. 5(September 2010-October 2010): 97-108.
- Meyer, Paul. "Cyber Security Through Arms Control: An Approach to International Co-Operation." *RUSI Journal: Royal United Services Institute for Defence Studies* 156, no. 2(April 2011-May 2011): 22-7.
- Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. "Internet Security and Networked Governance in International Relations." *International Studies Review* 15, no. 1(March 2013): 67-85.

- Nastasiu, Cătălin-Ionuț. "Cyber Security Strategies in the Internet Era." *Scientific Research & Education In The Air Force - AFASES* 2(2016): 619-24.
- Nielsen, Suzanne C. "Pursuing Security in Cyberspace: Strategic and Organizational Challenges." *Orbis: A Journal of World Affairs* 56, no. 3(Summer 2012): 336-56.
- Nissenbaum, Helen. "Where Computer Security Meets National Security." *Ethics and Information Technology* 7, no. 2(June 2005): 61-73.
- Roesener, G., Carl Bottolfson, and Gerry Fernandez. "Policy for US Cybersecurity." *Air & Space Power Journal* 28, no. 6(November 2014-December 2014): 38-54.
- Rohozinski, Rafal. "PANEL 2: Information/Cyber Warfare and Territorial Sovereignty: The End of Defense?" *American Foreign Policy Interests Supplement*(January 2015-February 2015): 4-7.
- Schmitt, Michael N. "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law." *Virginia Journal Of International Law* 54, no. 3(August 2014): 698-732.
- Segura Serrano, Antonio. "Cybersecurity: Towards a Global Standard in the Protection of Critical Information Infrastructures." *European Journal of Law & Technology* 6, no. 3(2015): 1-24.
- Shea, Jamie. "How Is NATO Dealing With Emerging Security Challenges?" *Georgetown Journal Of International Affairs* 14, no. 2(Summer 2013-Fall 2013): 193-201.
- Skinner, Christian Parajon. "An International Law Response to Economic Cyber Espionage." *Connecticut Law Review* 46, no. 4(May 2014): 1165-207.
- Vacca, W. Alexander. "Military Culture and Cyber Security." *Survival* 53, no. 6(December 2011): 159-76.
- Warner, Michael. "Cybersecurity: A Pre-History." *Intelligence and National Security* 27, no. 5(October 2012): 781-99.
- Whyte, Christopher. "Power and Predation in Cyberspace." *Strategic Studies Quarterly* 9, no. 1(Spring 2015): 100-118.

VII. INTERNATIONAL RELATIONS INCLUDE CHINA AND RUSSIA

Books, Government Documents, and Report Literature

- Austin, Greg. *Cyber Policy in China*. China Today. Cambridge: Polity, 2014.
(HN 740 .Z9 I5623 2014)
- Austin, Greg and Gady Franz-Stefan. *Cyber Detente Between the United States and China*. Washington: EastWest Institute, 2012.
(<https://www.eastwest.ngo/idea/cyber-detente-between-united-states-and-china>)
- Betz, David J. and Timothy C Stevens. *Cyberspace and the State: Towards a Strategy for Cyberpower*. Abingdon; New York: Routledge, 2011.
(HM 851 .B485 20141)
- Caton, Jeffrey L. *Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, and Response Implications*. Carlisle Barracks: U.S. Army War College, Strategic Studies Institute, 2014.
(REPORT LITERATURE ADA610-736)
(<http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA610736>)
- Costigan, Sean S., and Jake Perry, eds. *Cyberspaces and Global Affairs*. Burlington: Ashgate, 2012.
(JZ 1254 .C73 2012)
- Hagestad, William T. II. *21st Century Chinese Cyberwarfare: An Examination of the Chinese Cyberthreat from Fundamentals of Communist Policy Regarding Information Warfare through the Broad Range of Military, Civilian and Commercially Supported Cyberattack Threat Vectors*. Ely, Cambridgeshire: IT Governance, 2012.
(HV 6773 .H33 2012)
- Inkster, Nigel. *China's Cyber Power*. Adelphi, 456. Abington; London: Routledge; International Institute for Strategic Services, 2016.
(U 162 .A23 no. 456)
- Kremer, Jan-Frederik, and Benedikt Müller, eds. *Cyberspace and International Relations: Theory, Prospects and Challenges*. London: Springer, 2014.
- Lindsay, Jon R., Tai Ming Cheung, and Derek S. Revere, eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. New York: Oxford UP, 2015.
(HV 6773.15 .C97 C45 2015eb)
- Lord, Kristin M., Travis Sharp, and Robert E. Kahn, eds. *America's Cyber Future: Security and Prosperity in the Information Age (Volume II)*. Washington: Center for a New American Security, 2011.
(On order)
- Maness, Ryan C. and Brandon Valeriano. *Russia's Coercive Diplomacy: Energy, Cyber, and Maritime Policy As New Sources of Power*. Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan, 2015.
(HD 9502 .R83 V35 2015eb)

Nye, Joseph S. *The Future of Power*. New York: PublicAffairs, 2011.
(JC 330 .N92 2011)

Olagbemiro, Albert O. *Cyberspace As a Complex Adaptive System and the Policy and Operational Implications for Cyber Warfare*. Leavenworth: Army Command and General Staff College, School of Advanced Military Studies, 2014.
(REPORT LITERATURE)
(<http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA611977>)

Steinberg, James and Michael E. O'Hanlon. *Strategic Reassurance and Resolve: U.S - China Relations in the Twenty-First Century*. Princeton: Princeton UP, 2014.
(E 183.8 .C5 S84 2014)

Ventre, Daniel. *Cyber Conflict: Competing National Perspectives*. London; Hoboken: ISTE; John Wiley, 2012.
(HV 6773.15 .C97 C66 2012)

Ventre, Daniel, ed. *Chinese Cybersecurity and Defense*. Information systems, web and pervasive computing series. London: ISTE, 2014.
(QA 76.9 .A25 C456 2014eb)

JOURNALS

Broggi, Jeremy J. "Building on Executive Order 13636 to Encourage Information Sharing for Cybersecurity Purposes." *Harvard Journal of Law & Public Policy* 37, no. 2(Spring 2014): 653-76.

Buckerfield de la Roche, Alixe. "The Merger of Two Global Commons: The Need for New Governance." *Space Policy* 29, no. 2(May 2013): 159-63.

Cai, Cuihong and Diego Dati. "Words Mightier Than Hacks: Narratives of Cyberwar in the United States and China." *Asian Perspective: SPECIAL ISSUE* 39, no. 3(July 2015-September 2015): 541-53.

Chansoria, Monika. "Defying Borders In Future Conflict In East Asia: Chinese Capabilities In The Realm Of Information Warfare And Cyber Space." *The Journal of East Asian Affairs* 26, no. 1(Spring 2012): 105-27.

Choucri, Nazli and Daniel Goldsmith. "Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security." *Bulletin of the Atomic Scientists* 68, no. 2(March 2012): 70-8.

Demchak, Chris C. and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* 5, no. 1(Spring 2011): 32-61.

Demidov, Oleg. "Cyberwarfare and Russian Style of Cyberdefense." *Security Index: A Russian Journal on International Security* 19, no. 3(September 2013): 67-71.

Ebert, Hannes and Tim Maurer. "Contested Cyberspace and Rising Powers." *Third World Quarterly* 34, no. 6(July 2013): 1054-74.

- Forsyth Jr, James Wood. "What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace." *Strategic Studies Quarterly* 7, no. 1(Spring 2013): 93-113.
- Forsyth Jr., James Wood and Maj Billy Pope. "Structural Causes and Cyber Effects Why International Order Is Inevitable in Cyberspace." *Strategic Studies Quarterly* 8, no. 4(Winter 2014): 112-28.
- Forsyth Jr., James Wood and Maj Billy E. Pope. "Structural Causes and Cyber Effects: A Response to Our Critics." *Strategic Studies Quarterly* 9, no. 2(Summer 2015): 99-106.
- Gompert, David C. and Martin Libicki. "Cyber Warfare and Sino-American Crisis Instability." *Survival* 56, no. 4(August 2014-September 2014): 7-22.
- Goode, Andrea C. "Cyberterrorists: The Identification and Classification of Non-State Actors Who Engage in Cyber-Hostilities." *Military Law Review* 223(2015): 157-97.
- Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4, no. 3(Fall 2010): 102-35.
- Gärtner, Heinz. "Deterrence, Disarmament and Arms Control." *International Politics* 51, no. 6(November 2014): 750-762.
- Han, Rongbin. "Defending the Authoritarian Regime Online: China's "Voluntary Fifty-Cent Army"." *The China Quarterly* 224(October 2015): 1006-25.
- Hurwitz, Roger. "The Play of States: Norms and Security in Cyberspace." *American Foreign Policy Interests* 36, no. 5(September 2014-October 2014): 322-31.
- Kello, Lucas. "The Meaning of the Cyber Revolution." *International Security* 38, no. 2(Fall 2013): 7-40
- . "Correspondence: (Meaning of the Cyber Revolution)." *International Security* 39, no. 2(Fall 2014): 188-92.
- Kshetri, Nir. "Cybercrime and Cyber-Security Issues Associated With China: Some Economic and Institutional Considerations." *Electronic Commerce Research* 13, no. 1(March 2013): 41-69.
- Lin, Herbert. "China As an Ally in Cyberspace? How Washington and Beijing Could Make Common Cause Toward a Secure Online World." *Hoover Digest: Research & Opinion on Public Policy* 1(Winter 2016): 44-8.
- Lindsay, Jon R. "The Impact of China on Cybersecurity Fiction and Friction." *International Security* 39, no. 3(Winter 2014): 7-47.
- . "Inflated Cybersecurity Threat Escalates US-China Mistrust." *NPQ: New Perspectives Quarterly* 32, no. 3(July 2015): 17-21.
- Lindsay, Jon R. and Lucas Kello. "Correspondence: A Cyber Disagreement." *International Security* 39, no. 2(Fall 2014): 181-87.
- Malawer, Stuart S. "Chinese Economic Cyber Espionage: U.S. Litigation in the WTO and Other Diplomatic Remedies." *Georgetown Journal Of International Affairs* (Fall 2015): 158-67.

- Matsubara, Mihoko. "Countering Cyber-Espionage and Sabotage." *RUSI Journal* 15, no. 1(March 2014): 86-93.
- Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. "Internet Security and Networked Governance in International Relations." *International Studies Review* 15, no. 1(March 2013): 67-85.
- Nocetti, Julien. "Contest and Conquest: Russia and Global Internet Governance." *International Affairs* 91, no. 1(January 2015): 110-30.
- Peng, S. Y. "Cybersecurity Threats and the WTO National Security Exceptions." *Journal of International Economic Law* 18, no. 2(June 2015): 449-78.
- Ridout, Tim. "Building a Comprehensive Strategy of Cyber Defense, Deterrence, and Resilience." *The Fletcher Forum of World Affairs* 40, no. 2(Summer 2016): 63-83.
- Roberts, Kerry V. "SUN TZU and The Art of Cyber Warfare." *Journal of Counterterrorism & Homeland Security International* 19, no. 1(Spring 2013): 12-4.
- Segal, Adam. "The Code Not Taken: China, the United States, and the Future of Cyber Espionage." *Bulletin of the Atomic Scientists* 69, no. 5(September 2013): 38-45.
- Segal, Adam M. "Cyberspace: The New Strategic Realm in US–China Relations." *Strategic Analysis* 38, no. 4(July 2014): 577-81.
- Slack, Chelsey. "Wired Yet Disconnected: The Governance of International Cyber Relations." *Global Policy* 7, no. 1(February 2016): 69-78.
- Stytz, Martin R., and Sheila B. Banks. "Toward Attaining Cyber Dominance." *Strategic Studies Quarterly* 8, no. 1(Spring 2014): 55-87.
- Vaishnav, Chintan, Nazli Choucri, and David Clark. "Cyber International Relations As an Integrated System." *Environment Systems and Decisions* 33, no. 4(December 2013): 561=76.
- Van Epps, Geoff. "Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain." *Connections* 12, no. 4(Fall 2013): 15-50.
- Yakushev, Mikhail. "Identity in Cyberspace: Towards a Global Impact." *Security Index: A Russian Journal On International Security* 18, no. 4(December 2012): 33-44.
- Young-do, K., K Jin-sung, and L Kyung-ho. "Major Issues of the National Cyber Security System in South Korea, and Its Future Direction." *Korean Journal of Defense Analysis* 25, no. 4(December 2013): 435-55.

VIII. LEGAL REGULATIONS AND IMPLICATIONS

Books, Government Documents, and Report Literature

- Ohlin, Jens David, Kevin Govern, and Claire Oakes Finkelstein, eds. *Cyber War: Law and Ethics for Virtual Conflicts*. Oxford: Oxford UP, 2015.
(KZ 6718 .C93 2015)
- Saxon, Dan, ed. *International Humanitarian Law and the Changing Technology of War*. International Humanitarian Law Series. Leiden : Martinus Nijhoff, 2013.
- Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge UP, 2013.
(KZ 6718 .T35 2013eb)
- Spinello, Richard A. *Cyberethics: Morality and Law in Cyberspace*. 6th ed. Burlington: Jones & Bartlett, 2017.
(TK 5105.875 .I57 S68 2017)
- Taddeo, Mariarosaria and Luciano Floridi. *The Ethics of Information Warfare*. Cham Switzerland: Springer, 2014.

JOURNALS

- Banks, William. "The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber Warfare." *International Law Studies* 89(2013): 156-97.
- Brown, Davis. "A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict." *Harvard International Law Journal* 47, no. 1(Winter 2006): 179-221.
- Brown, Gary and Keira Poellet. "The Customary International Law of Cyberspace." *Strategic Studies Quarterly* 6, no. 3(Fall 2012): 126-45.
- Brown, Gary D. and Andrew O. Metcalf. "Easier Said Than Done: Legal Reviews of Cyber Weapons." *Journal of National Security Law & Policy* 7, no. 1(February 2014): 115-38.
- Crane, David M. "Fourth Dimensional Intelligence Thoughts on Espionage, Law, and Cyberspace." *International Law Studies* 76(2002): 311-21.
- Dinstein, Yoram. "Computer Network Attacks and Self-Defense." *International Law Studies* 76, no. 1(2000): 99-119.
- Droege, Cordula. "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians." *International Review of the Red Cross* 94, no. 886(June 2012): 533-78.
- Dunlap Jr., Charles J. "Perspectives for Cyber Strategists on Law for Cyberwar." *Strategic Studies Quarterly* 5, no. 1(Spring 2011): 81-99.
- . "Some Reflections on the Intersection of Law and Ethics in Cyber War." *Air & Space Power Journal* 27, no. 1(January 2013-February 2013): 22-43.

- Eichensehr, Kristen E. "The Cyber-Law of Nations." *Georgetown Law Journal* 103, no. 2(January 2015): 317-80.
- . "Cyberwar & International Law Step Zero." *Texas International Law Journal* 50, no. 2(2015): 355-78.
- Franzese, Patrick W. "Sovereignty in Cyberspace: Can It Exist." *Air Force Law Review* 64(2009): 1-42.
- Gervais, Michael. "Cyber Attacks and the Laws of War." *Berkeley Journal Of International Law* 30, no. 2(2012): 525-79.
- Gill, Terry D. and Paul A. L. Ducheine. "Anticipatory Self-Defense in the Cyber Context." *International Law Studies* 89(2013): 438-71.
- Glennon, Michael J. "The Road Ahead: Gaps, Leaks and Drips." *International Law Studies* 89(2013): 362-86.
- Goldsmith, Jack. "How Cyber Changes the Laws of War." *European Journal of International Law* 24, no. 1(February 2013): 129-38.
- Goldsmith, Jack L. "The Internet and the Abiding Significance of Territorial Sovereignty." *Indiana Journal of Global Legal Studies* 5, no. 2(Spring 1998): 475-91.
- Graham, David E. "Cyber Threats and the Law of War." *Journal of National Security Law & Policy* 4, no. 1(2010): 87-102.
- Gross, Jessica R. "Hacked and Be Hacked: A Framework for the United States to Respond to Non-State Actors in Cyberspace." *California Western International Law Journal* 46, no. 2(Spring 2016): 109-45.
- Gross, Oren. "Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents." *Cornell International Law Journal* 48, no. 3(Fall 2015): 481-511 .
- Heidenreich, John. "The Privacy Issues Presented by the Cybersecurity Information Sharing Act." *North Dakota Law Review* 91, no. 2(2015): 395-410.
- Heintschel von Heinegg, Wolff. "Territorial Sovereignty and Neutrality in Cyberspace." *International Law Studies* 89(2013): 123-56.
- Hollis, Duncan B. "An E-SOS for Cyberspace." *Harvard International Law Journal* 52, no. 2(Summer 2011): 373-432.
- . "Why States Need an International Law for Information Operations." *Lewis & Clark Law Review* 11, no. 4(Winter 2007): 1023-61.
- Jensen, Eric Talbot. "Cyber Sovereignty: The Way Ahead." *Texas International Law Journal* 50, no. 2(2015): 273-302.
- . "Sovereignty and Neutrality in Cyber Conflict." *Fordham International Law Journal* 35, no. 3(2012): 814-41.

- Johnson, Phillip A. "Is It Time for a Treaty on Information Warfare?" *International Law Studies* 76, (2002): 439-455.
- Kanuck, Sean. "Sovereign Discourse on Cyber Conflict under International Law." *Texas Law Review* 88, no. 7(June 2010): 1571-597.
- Keen, Major Jason F. "Conventional Military Force As a Response to Cyber Capabilities on Sending Packets and Receiving Missiles." *Air Force Law Review* 73(2015): 111-50.
- Kesan, Jay P. and Carol M. Hayes. "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace." *Harvard Journal of Law & Technology* 25, no. 2(Spring 2012): 415-529.
- Liaropoulos, Andrew. "Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction?" *Proceedings of the International Conference on Information Warfare & Security* (March 2013): 136-40.
Call Number
http://www.academia.edu/3322607/Exercising_State_Sovereignty_in_Cyberspace_an_international_cyber-order_under_construction_in_8th_International_Conference_on_Information_Warfare_and_Security_Denver_Colorado_25-26_March_2013)
- Lin, Herbert. "Cyber Conflict and International Humanitarian Law." *International Review of the Red Cross* 94, no. 886(June 2012): 515-31.
- Lotrionte, Catherine. "Countering State-Sponsored Cyber Economic Espionage under International Law." *North Carolina Journal Of International Law And Commercial Regulation* 40, no. 2(Winter 2015): 443-541.
- Messerschmidt, Jan E. "Hackback: Permitting Retaliatory Hacking by Non-State Actors As Proportionate Countermeasures to Transboundary Cyberharm." *Columbia Journal of Transnational Law* 52, no. 1(2013): 275-324.
- Murphy, John F. "Computer Network Attacks by Terrorists: Some Legal Dimensions." *International Law Studies* 76(2002): 323-51.
- O'Donnell, Brian T. and James C. Kraska. "International Law of Armed Conflict and Computer Network Attack: Developing the Rules of Engagement." *International Law Studies* 76(2002): 395-419.
- Pagallo, Ugo. "Cyber Force and the Role of Sovereign States in Information Warfare." *Philosophy and Technology* 28, no. 3(September 2015): 407-25.
- Rinear, Matthew. "Armed with a Keyboard: Presidential Directive 20, Cyber-Warfare, and the International Laws of War." *Capital University Law Review* 43, no. 3(Summer 2015): 679-720.
- Rishikof, Harvey and Bernard Horowitz. "Shattered Boundaries: Whither the Cyber Future." *Journal of Military and Strategic Studies* 14, no. 2(2012): 1-18.
- Santos, Lino. "Cyberspace Regulation: Cesurists and Traditionalists." *Janus.Net: E-Journal of International Relations* 6, no. 1(May 2015-October 2015): 86-99.

- Schmitt, Michael N. "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law." *Virginia Journal Of International Law* 54, no. 3(August 2014): 698-732.
- . "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Columbia Journal of Transnational Law* 37, no. 3(1999): 885-937.
- . "The Law of Cyber Warfare: Quo Vadis?" *Stanford Law & Policy Review* 25(2014): 269-99.
- . "Rewired Warfare: Rethinking the Law of Cyber Attack." *International Review of the Red Cross* 96, no. 893(March 2014): 189-206.
- . "Wired Warfare: Computer Network Attack and Jus in Bello." *International Review of the Red Cross*, 84, no. 846(June 2002): 365-99.
- Schmitt, Michael N. and Sean Watts. "The Decline of International Humanitarian Law *Opinio Juris* and the Law of Cyber Warfare." *Texas International Law Journal* 50, no. 2(2015): 189-231.
- Serrano, Antonio Segura. "Cybersecurity: Towards a Global Standard in the Protection of Critical Information Infrastructures." *European Journal of Law and Technology* 6, no. 3(2015): 1-121.
- Shackelford, Scott J. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal Of International Law* 27, no. 1(2009): 192-251.
- Smith, Jeffrey H. and Gordon N. Lederman. "Weapons Like to Lightning"! US Information Operations and US Treaty Obligations." *International Law Studies* 76(2002): 375-93.
- Walker, George K. "Neutrality and Information Warfare." *International Law Studies* 76(2002): 233-63.
- Williams, Robert D. "(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action." *George Washington Law Review* 79, no. 4(June 2011): 1162-200.
- Zekos, Georgios I. "Demolishing State's Sole Power over Sovereignty and Territory Via Electronic Technology and Cyberspace." *Journal of Internet Law* 17, no. 5(November 2013): 3-17.

IX. FINANCIAL AND ECONOMIC AREAS JOURNALS

- Balitzer, Stephanie. "What Common Law and Common Sense Teach Us About Corporate Cybersecurity." *University Of Michigan Journal of Law Reform* 49, no. 4(2016): 891-919.
- Balushi, Taiseera Al, Saqib Ali, and Osama Rehman. "Economics of Cyber Security and the Way Forward." *International Journal of Cyber Warfare & Terrorism* 6, no. 4(October 2016-December 2016): 41-57.
- Baumbauer, Derek E. "Ghost in the Network." *University Of Pennsylvania Law Review* 162, no. 5(April 2014): 1011-91.
- Daniali, Ghorban. "E-Money Laundering Prevention." *New Marketing Research Journal*, Special Issue(2014): 29-38.
- Dobrian, Joseph. "Are You Sitting on a Cyber Security Bombshell?" *Journal of Property Management* 80, no. 5(September 2015-October 2015): 8-11.
- Foster, William and Hannah Thoreson. "How to Create a World Financial Community Resilient to Cyber-Espionage and Hacking?" *Security Index: A Russian Journal on International Security* 19, no. 4(December 2013).
- Jackson, Aaron, Drake P. Saffell, and Brian D. Fitzpatrick. "The Evolving Financial Services Industry: The Financial Advisory Role Today and in the Future." *Journal of Business Inquiry: Research, Education & Application* 15, no. 1(2016): 17-32.
- Kshetri, Nir. "Cybercrime and Cyber-Security Issues Associated with China: Some Economic and Institutional Considerations." *Electronic Commerce Research* 13, no. 1(March 2013): 41-69.
- Lotrionte, Catherine. "Countering State-Sponsored Cyber Economic Espionage under International Law." *North Carolina Journal of International Law And Commercial Regulation* 40, no. 2(Winter 2015): 443-541.
- Malawer, Stuart S. "Chinese Economic Cyber Espionage: U.S. Litigation in the WTO and Other Diplomatic Remedies." *Georgetown Journal of International Affairs* (Fall 2015): 158-67.
- Manley, Max. "Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership." *Journal of Strategic Security* 8, no. 5(2015): 85-98.
- Skinner, Christian Parajon. "An International Law Response to Economic Cyber Espionage." *Connecticut Law Review* 46, no. 4(May 2014): 1165-207.
- Westfall, Skip. "Be Prepared." *Financial Executive* 31, no. 2(Spring 2015): 46-51.
- Whyte, Christopher. "Developed States' Vulnerability to Economic Disruption Online." *Orbis* 60, no. 3(Summer 2016): 417-32.

Wortham, Anna. "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?" *Federal Communications Law Journal* 64, no. 3(May 2012): 643-60.

X. CYBERWARFARE

Books, Government Documents, and Report Literature

- Andress, Jason and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. 2nd ed. Waltham: Syngress, 2014.
(U163 .A64 2014 eb)
- Andress, Jason, Steve Winterfeld, and Russ Rogers. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Boston: Elsevier, 2011.
(U 163 .A64 2011)
- Arquilla, John, and Douglas A. Borer, eds. *Information Strategy and Warfare : A Guide to Theory and Practice*. London: Routledge, 2007.
(On order)
- Bryant, William D. *International Conflict and Cyberspace Superiority: Theory and Practice*. Routledge Studies in Conflict, Security and Technology. London: Routledge, 2015.
(HM 851 .B79 2016eb)
- Clarke, Richard A. and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco, 2012.
(HV 6773.2 .C53 2010)
- Demchak, Chris C. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Studies in security and international affairs. Athens: U of Georgia P, 2011.
(U 163 .D36 2011)
- Friis, Karsten, and Jens Ringsmose, eds. *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*. Routledge studies in conflict, security and technology. London; New York: Routledge, Taylor & Francis Group, 2016.
(U 163 .C6254 2016eb)
- Green, James A. *Cyber Warfare: A Multidisciplinary Analysis*. Routledge studies in conflict security and technology. London: Routledge, 2015
(U 163 .C936 2015)
- Healey, Jason ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, VA: Cyber Conflict Studies Association, 2013.
(HV 6773.15 .C97 F54 2013)
- Heintze, Hans-Joachim, and Pierre Thielbörger, eds. *From Cold War to Cyber War: The Evolution of the International Law of Peace and Armed Conflict Over the Last 25 Years*. Berlin: Cham Springer, 2016.
- Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND, 2009.
(REPORT LITERATURE RAND M6-877-AF) (<http://www.rand.org/pubs/monographs/MG877/>)
- Mazanec, Brian M. *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. Lincoln: U of Nebraska P, 2015.
(KZ 6718 .M39 2015)

- Powers, Shawn M. and Michael Jablonski. *The Real Cyber War: The Political Economy of Internet Freedom*. The History of communication. Urbana: U of Illinois P, 2015.
(HM 851 .P6878 2015)
- Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge: MIT P, 2001.
(U 163 .R24 2001)
- Reveron, Derek S., ed. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington: Georgetown UP, 2012.
(HV 6773.15 .C97 C93 2012)
- Saxon, Dan, ed. *International Humanitarian Law and the Changing Technology of War*. International Humanitarian Law Series. Leiden : Martinus Nijhoff, 2013.
- Shakarian, Jana and Andrew Ruef. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Amsterdam; Boston: Syngress, 2013.
(U 163 .S438 2013)
- Springer, Paul J. *Cyber Warfare: A Reference Handbook*. Contemporary world issues. Santa Barbara: ABC-CLIO, 2015.
(U 163 .S66 2015)
- Valeriano, Brandon and Ryan C. Maness. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford; New York: Oxford UP, 2015.
(U 163 .V36 2015)

JOURNALS

- Applegate, Scott. "Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare." *IEEE Security & Privacy Magazine* 9, no. 5(May 2011): 16-22.
- Armenchev, Ilina, and Stefko Smolenov. "From Real Cyber Conflict Through Wishful Cyber Security to (Un) Likely Cyber Peace." *Revista Academiei Fortelor Terestre* 20, no. 3(September 2015): 259-66.
- Arquilla, John. "Twenty Years of Cyberwar." *Journal of Military Ethics* 12, no. 1(April 2013): 80-87.
- Arquilla, John and David Ronfeldt. "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2(1993): 141-65.
- Banks, William. "The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber Warfare." *International Law Studies* 89(2013): 156-97.
- Brown, Davis. "A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict." *Harvard International Law Journal* 47, no. 1(Winter 2006): 179-221.

- Brown, Gary D. and Andrew O. Metcalf. "Easier Said Than Done: Legal Reviews of Cyber Weapons." *Journal of National Security Law & Policy* 7, no. 1(February 2014): 115-38.
- Cser, Orsolya. "The Role and Security of Money From the Aspect of Cyber Warfare." *AARMS: Academic & Applied Research in Military & Public Management Science*. 14, no. 3(January 2015): 331-42.
- Danks, David and Joseph H. Danks. "The Moral Permissibility of Automated Responses during Cyberwarfare." *Journal of Military Ethics* 12, no. 1(April 2013): 18-33.
- Dev, Priyanka R. ""Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response." *Texas International Law Journal* 50, no. 2(2015): 379-99.
- Drmola, Jakub. "Looking for Insurgency in Cyberspace." *Central European Journal Of International & Security Studies* 8, no. 4(December 2014): 56-77.
- Droege, Cordula. "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians." *International Review of the Red Cross* 94, no. 886(June 2012): 533-78.
- Dunlap, Jr. Charles J. "Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy." *International Law Studies* 76(2002): 353-73.
- Durante, Massimo. "Violence, Just Cyber War and Information." *Philosophy & Technology* 28, no. 3(September 2015): 369-85.
- Eberle, Christopher J. "Just War and Cyberwar." *Journal of Military Ethics* 12, no. 1(April 2013): 54-67.
- Fiedler, James D. "Bandwidth Cascades: Escalation and Pathogen Models for Cyber Conflict Diffusion." *Small Wars Journal* 24(2013).
- Gartzke, Erik. "The Myth of Cyberwar." *International Security* 38, no. 2(Fall 2013): 41-73.
- Gartzke, Erik and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24, no. 2(April 2015-June 2015): 316-48.
- Geers, Kenneth. "Cyber Weapons Convention." *Computer Law & Security Review* 26, no. 5(September 2010): 547-51.
- Geiss, Robin. "Cyber Warfare: Implications for Non-International Armed Conflicts." *International Law Studies* 89(2013): 627-45.
- Geiss, Robin and Henning Lahmann. "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space." *Israel Law Review* 45, no. 3(November 2012): 381-99.
- Goldsmith, Jack. "How Cyber Changes the Laws of War." *European Journal Of International Law* 24, no. 1(February 2013): 129-38.
- Graham, David E. "Cyber Threats and the Law of War." *Journal of National Security Law & Policy* 4, no. 1(2010): 87-102.

- Halpern, Sue. "US Cyber Weapons: Our "Demon Pinball"." *New York Review of Books* 63, no. 14(September 2016): 26-30.
Call Number: "Zero Days" film
- Hauck, Erica. "The Cloud of War: Securing the Operational Domain of Cyberspace With a Robust Military Command." *Northern Kentucky Law Review* 41, no. 3(2014): 515-34.
- Huntley, Wade L. "Strategic Implications of Offense and Defense in Cyberwar. Koloa HI." *2016 49th Hawaii International Conference on System Sciences (HICSS)* (January 2016): 5588-595.
- Jensen, Eric Talbot. "Cyber Warfare and Precautions Against the Effects of Attacks." *Texas Law Review* 88, no. 7(June 2010): 1533-69.
- Junio, Timothy J. "How Probable Is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate." *Journal of Strategic Studies* 36, no. 1(February 2013): 125-33.
- Kanuck, Sean. "Sovereign Discourse on Cyber Conflict Under International Law." *Texas Law Review* 88, no. 7(June 2010): 1571-597.
- Kello, Lucas. "The Meaning of the Cyber Revolution." *International Security* 38, no. 2(Fall 2013): 7-40.
- Lewis, James. "Cyberwar Thresholds and Effects." *IEEE Security & Privacy Magazine* 9, no. 5(March 2011): 23-9.
- Libicki, Martin C. "Why Cyber War Will Not and Should Not Have Its Grand Strategist." *Strategic Studies Quarterly* 8, no. 1(Spring 2014): 23-39.
- Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35, no. 3(May 2012): 401-28.
- Lin, Herbert. "Cyber Conflict and International Humanitarian Law." *International Review of the Red Cross* 94, no. 886(June 2012): 515-31.
- Martemucci, Matteo G. "Unpunished Insults--The Looming Cyber Barbary Wars." *Case Western Reserve Journal Of International Law* 47, no. 3(Spring 2015): 53-62.
- McReynolds, Phillip. "How to Think About Cyber Conflicts Involving Non-State Actors." *Philosophy and Technology* 28, no. 3(June 2015): 427-48.
- Peterson, Dale. "Offensive Cyber Weapons: Construction, Development, and Employment." *Journal of Strategic Studies* 36, no. 1(February 2013): 120-24.
- Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1(2012): 5-32.
- Rid, Thomas and Peter McBurney. "Cyber-Weapons." *The RUSI Journal* 157, no. 1(February 2012): 6-13.
- Rinear, Matthew. "Armed With a Keyboard: Presidential Directive 20, Cyber-Warfare, and the International Laws of War." *Capital University Law Review* 43, no. 3(Summer 2015): 679-720.
- Saltzman, Ilai Z. "Cyber Posturing and the Offense-Defense Balance." *Contemporary Security Policy* 34, no. 1(March 2013): 40-63.

- Schmitt, Michael N. "Classification of Cyber Conflict." *International Law Studies* 89(2013): 233-51.
- . "The Law of Cyber Warfare: Quo Vadis?" *Stanford Law & Policy Review* 25(2014): 269-99.
- Sklerov, Matthew J. "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent." *Military Law Review* 201(Fall 2009): 1-85.
- Theohary, Catherine A. and John W. Rollins. *Cyberwarfare and Cyberterrorism: In Brief*. Washington: Congressional Research Service, 2015.
Call Number: (fas.org/sgp/crs/natsec/R43955.pdf)
- Valeriano, Brandon and Ryan C Maness. "The Dynamics of Cyber Conflict between Rival Antagonists." *Journal of Peace Research* 53, no. 1(May 2014): 347-60.
- Waxman, Matthew C. "Cyber-Attacks and the Use of Force: Back to the Future." *Yale Journal of International Law* 36(Summer 2011): 421-59.
- Whyte, Christopher. "Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea." *Comparative Strategy* 35, no. 2(2016): 93-102.
- Wortham, Anna. "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?" *Federal Communications Law Journal* 64, no. 3(May 2012): 643-60.

XI. WEBSITES AND PDFs

Atlantic Council: Working Together to Secure the Future. Washington: 1961.

Call Number: (<http://www.atlanticcouncil.org/search?searchword=cyber&searchphrase=all>)

Healey, Jason. *Beyond Attribution: Seeking National Responsibility for Cyber Attacks.* Issue brief. Washington: Atlantic Council, 2012.

(http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF)

Hutchins, Eric M., Michael J. Clopperty, and Rohan M. Amin . *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* Bethesda: Lockheed Martin, 2014.

(<http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>)

Landwehr, Carl E. *History of US Government Investments in Cybersecurity Research: A Personal Perspective.* Oakland: 2010 IEEE Symposium on Security and Privacy, 2010.

(<http://ieeexplore.ieee.org/document/5504783/>)

Lewis, James A. *Conflict and Negotiation in Cyberspace.* CSIS Technology and Public Policy Program. Washington: Center for Strategic and International Studies, 2013:

(http://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf)

Sangbae Kim. *Policy Recommendation for South Korea's Middle Power Diplomacy: Cyber Security.* Seoul: Seoul National University, 2015.

(http://www.eai.or.kr/data/bbs/eng_report/201503121530342.pdf)

Van der Meer, Sico. *Foreign Policy Responses to International Cyber-Attacks.* Den Haag: Clingendael (Netherlands Institute of International Relations), 2015.

(http://www.clingendael.nl/sites/default/files/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf)

---. *Signalling As a Foreign Policy Instrument to Deter Cyber Aggression.* Den Haag: Clingendael Netherlands Institute of International Relations, 2015.

(http://www.clingendael.nl/sites/default/files/PB_Signalling_as_a_foreign_policy_instrument_SvdM.pdf)